UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/576,975	04/20/2006	Holger Krummel	851.0015.U1(US)	8160

29683 7590 02/03/2009

HARRINGTON & SMITH, PC
4 RESEARCH DRIVE, Suite 202
SHELTON, CT 06484-6212

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
02/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/576,975	KRUMMEL ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30,34 and 35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30,34 and 35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 December 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/576,975 is presented for examination by the examiner. Claims 1-30 are amended, 31-33 canceled and 34-35 are added.

Response to Amendment

Drawings

Examiner accepts the newly submitted drawings and therefore withdraws the objection.

Claim Objections

The presently filed claim amendments overcome the claim objections.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

The presently filed claim amendments overcome the previous rejection of claims 3, 4, 16, and 17.

Claims 21 and 22 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The amendment has not corrected these claims' deficiencies. Both claim 21 and 22 still recite the limitation "the received signal" which lacks antecedent basis. As per claim 23, which is dependent on claim 22, is similarly rejected for at least the same reason as claim 22.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 35 Is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. In order for claims directed to memory which stores computer readable instructions it must be clear that it is the processor which executes those instructions on the media. The processor is the only intelligent device which can execute those instructions thereby causing an action to occur other than software manipulation.

Response to Arguments

Examiner has fully considered both Applicant's arguments and affidavit filed on 12/4/08. The affidavit filed on 12/4/08 under 37 CFR 1.131 has been

considered but is ineffective to overcome the USP Application Publication 2005/0021940 to "Ma" reference.

The evidence submitted is insufficient to establish a conception of the invention prior to the effective date of the 6-13-03 reference. While conception is the mental part of the inventive act, it must be capable of proof, such as by demonstrative evidence or by a complete disclosure to another. Conception is more than a vague idea of how to solve a problem. The requisite means themselves and their interaction must also be comprehended. See *Mergenthaler v. Scudder*, 1897 C.D. 724, 81 O.G. 1417 (D.C. Cir. 1897). Applicant submitted alleged evidence of conception by a signed invention report. This report was signed by the inventors on 5-26-03. This is the only submitted evidence which predates the Ma reference which has a US filing date of 6-13-03. However, proof of invention is lacking in this document as detailed below.

Only the first 5 sections have any comments about the invention. Specifically under section 4, a statement is made about the idea of the invention. The concept which is present merely describes a system in which a passkey is entered one time into all the members of a network, master and slaves inclusive. Then it states that if a new device joins, the master will try to authenticate with it but it if fails both will need to be inputted with the passkey. This does not sound echo the claimed invention nor is there any indication how a "new" device gets the passkey without some type of user input whether it is by hand input or voice input. Now looking first at only claim 1, the inventive concept here is making a stored secret available at a first apparatus without contemporaneous user input. The underlying concept behind this is that somehow this

stored secret is put into the first apparatus without user input. If the first apparatus corresponds to the new device from the invention report, the only way of inputting the secret is by user input. According to the invention report, the master will try the [inputted] passkey. There is no underlying implication that the master would send the passkey, because the master must authenticate the slave. Therefore it is the slave which must present some form of authenticating evidence such as a passkey. From the invention report, it seems that if a secret must be inputted into the slave at some point. The claimed concept does not carry this same idea. Claim 1 rather emphasizes (without explanation) that the new device receives the secret without any input at that time. This is in stark contrast from the invention report, wherein the secret must be entered into both the slave and master. Therefore it does not appear that the invention report of 5-26-03 supports the claimed invention. The invention report is void of providing more than a vague idea of how to solve a problem. Not only does the invention concept not provide disclosure of the claimed invention, the vagueness does not even appear to address the same inventive concept. The other claims only provide for more details which are not support by the invention report. There is not sufficient evidence on the single paper, page 2, of the invention report to support invention conception on 5-26-03. That being the only document preceding Ma, Examiner must maintain the previous rejection on the grounds that Ma is prior art. However, the evidence seems to support due diligence and reduction to practice from July of 2003 to the filing date. If more evidence of conception of invention is submitted it will require further consideration.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-24, 26-30, and 34-35 are rejected under 35 U.S.C. 102(e) as being anticipated by USP Application Publication 2005/0021940 to Ma, hereinafter Ma.

As per claim 1, Ma teaches a method of joining a first device to a radio communications network controlled by a second device without contemporaneous user input of a secret at the second device [PIN is stored in second device], comprising: storing in the second device a secret generated at the second device [PIN stored in SIM]; making the stored secret available at the first device [user inputs PIN]; and creating in the first device and in the second device, using the secret, a secret key for use in securing communication between the first and second devices [secure pairing and wireless communication via one more keys and/or algorithms] (0032).

As per claim 2, Ma teaches the secret is previously generated at the second device by user input to the second device [PINs are chosen and stored in SIM card on smartphone] (0027 and 0033].

As per claim 3, Ma teaches the stored secret is associated with an operational mode of the device [allow for operation of service if PIN matches] (0033).

As per claim 4, Ma teaches wherein the stored secret is associated with a service provided by the device [allow for operation of service if PIN matches] (0033).

As per claim 5, Ma teaches receiving a signal from the first device and in response to the received signal, automatically creating without user intervention the secret key [automatic pairing of devices when correct PIN is received] (0039).

As per claim 6, Ma teaches making the stored secret available at the first device is without communication in the network [PIN is not transmitted from second device to first device, user of first device must know PIN in order to authenticate] (0039).

As per claim 7, Ma teaches making the stored secret available at the first device involves user input of the secret to the first device [user inputs PIN via input device] (0039).

As per claim 8, Ma teaches storing in the second device an identifier of the first device and an identifier of the second device [identifying information of the first device is stored in SIM of the second device for automatic pairing] (0039).

As per claim 9, Ma teaches the step of creating the secret key uses a random number communicated between the first and second devices [use of random number helps secure the authentication process] (0029).

As per claim 10, Ma teaches the step of creating the secret key uses an identifier of one of the first and second devices, communicated between the first and second devices, in the creation of the secret key [secure pairing using identifying information of the devices so that automatic pair can later occur simply when the two devices are in range of one another] (0037). Ma specifically mentions that the signal includes the identifying information.

As per claim 11, Ma teaches re-using the stored secret to join a third device to the radio communications network without contemporaneous user input of a secret at the second device, comprising: making the stored secret [PIN] available at the third device; and creating in the third device and in the second device, using the secret, a secret key for securing communication between the third and second devices [a plurality of devices can perform the same pairing to the second device as the first device] (0034).

As per claim 12, Ma teaches a method of joining a plurality of first devices to a radio communications network controlled by a second device, comprising: storing in the second device a generated secret [PIN] at the second device; making the stored secret available to each of the first devices [input by users of the plurality of first devices]; and creating in the first devices and in the second device, using the secret, at least one secret key [secure pairing via keys] for use in securing communication between the first devices and the second device (0032 and 0034).

As per claim 13, Ma teaches the step of creating at least one secret key comprises: creating a plurality of secret keys distributed across the first devices by

creating a different secret key at each of the plurality of first devices [secure channel (encrypted) are created between each device using identifying information from the first devices, therefore each key will be different for each device for obvious security reason] (0034);

and creating an identical plurality of secret keys at the second device [keys must match in order for communication to occur between two devices] (0037).

As per claim 14, Ma teaches a device [smartphone] (Fig. 3, 308) for controlling a radio communications network comprising the device and one or more additional devices, the device comprising: a user interface [keypad] for generating a secret [PIN] by user input; a memory [SIM] for storing a generated secret for use in securing communications in the network; a radio transceiver [in smartphone] for communicating in the network; and a processor for accessing the secret stored in the memory and for creating, using the accessed secret, a secret key for securing communication (0033).

As per claim 15, Ma teaches the stored secret is generated by user input using the user interface [smart phone has keyboard for entering PIN which is stored in SIM] (0037) It is inherent that the PIN was at some time prior to the pairing entered by the user and stored in the SIM.

As per claim 16, Ma teaches the stored secret is associated with an operational mode of the device [secret must be known in order to operate] (0033).

As per claim 17, Ma teaches wherein the stored secret is associated with a service provided by the device [secret must be known in order to gain service of the communication network] (0033).

As per claim 18, Ma teaches the radio transceiver [in smartphone] is operable to receive a signal from any one of the additional devices and the processor is operable to access the secret in the memory in response to the received signal and create the secret key (0038).

As per claim 19, Ma teaches the processor is operable to automatically create the secret key in response to the received signal [processor employs algorithms to the identifying data with keys to create a unique key] (0033).

As per claim 20, Ma teaches the stored secret [PIN] is independent of the origin of the received signal [the PIN is just made up by a user and stored in the SIM] (0032).

As per claim 21, Ma teaches the secret key is dependent upon the origin of the received signal [key is generated using identifying information of the first device, thus the key will depend on the device sending the signal] (0037).

As per claim 22, Ma teaches the received signal is a request (pairing request) and the secret key is dependent upon the content of the received request [key is generated using identifying information of the first device, thus the key will depend on the device sending the signal] (0037).

As per claim 23, Ma teaches the request includes a random value [number] used with at least the stored secret to create the secret key [first device passes random number to second device for authentication purposes which are an indication of usage] (0029).

As per claim 24, Ma teaches the processor is operable in a first mode to obtain a secret [PIN] by accessing the secret stored in the memory [SIM], is operable in a

second mode to obtain a secret by enabling user input of data [receives PIN from user], and is operable in the first mode and in the second mode to create, using the obtained secret, the secret key for securing communication (0037).

As per claim 26, Ma teaches the memory stores a device identifier [identifying information] for use with at least the stored secret to create the secret key (0037).

As per claim 27, Ma teaches a user input device [keypad] for programming the value of the stored secret [smart phone has keyboard for entering PIN which is stored in SIM] (0037) It is inherent that the PIN was at some time prior to the pairing entered by the user and stored in the SIM.

As per claim 28, Ma teaches the secret key is for use in securing all communications in the network [securely paired] (0032).

As per claim 29, Ma teaches the memory [SIM] is for storing a secret [PIN] for use in securing communications in the network between the device and a first additional device and between the device and a second additional device (0034), the processor is for accessing the secret in the memory and for creating, using the secret, a first secret key [key is created using identifying information of the first device] in common with the first additional device for securing communication between the device and the first additional device and a second secret key in common with the second additional device for securing communication between the device and the second additional device (0033). Ma teaches the process of securely pairing two devices can be extended to multiple devices, each carrying out their own secure pairing.

As per claim 30, Ma teaches a user interface for entering data [smart phone with keypad], wherein when the device participates in a different network controlled by a different device the user interface is usable to enter a secret stored at the different device and the processor is operable to create, using the entered secret, a secret key for securing communication (0032-0037). Ma teaches that the device holding the SIM card ultimately controls access to the wireless services. Ma teaches SIM are removable and can be transferred to other devices. Therefore when a control device gives up its SIM card, it can no longer function as the master device. This device then becomes the exemplary first device in the communication scheme. Ma teaches the first device gains access by secure pairing. It is therefore inherent that the smartphone without the SIM can perform the same authentication process that the PDA invokes as an example.

As per claim 34, Ma teaches a means for storing in a second apparatus which controls access to a radio communications network a secret generated at the second apparatus (0032);

means for making the stored secret available at a first apparatus without contemporaneous user input (0032); and

means for creating in the second apparatus, using the secret, a secret key for use in securing communication between the first and second apparatus (0032).

As per claim 35, Ma teaches a memory storing a program of computer readable instructions executable by a processor to perform actions directed to securing communication between a first and second apparatus, the actions comprising:

storing in a second apparatus which controls access to a radio communications network a secret generated at the second apparatus (0032);

making the stored secret available at a first apparatus without contemporaneous user input (0032); and

creating in the second apparatus, using the secret, a secret key for use in securing communication between the first and second apparatus (0032).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ma in view of USP Application Publication 2004/0043790 to Ben-David et al, hereinafter Ben-David.

As per claim 25, Ma does not explicitly teach the first mode is an interactive gaming mode and second mode is an idle mode. Ma teaches the use of PDA, smartphones, and the like to wirelessly communicate securely with others devices in

short range. Ben-David teaches that PDA has numerous operating modes such as a gaming mode (0102) and sleep (idle) mode (0298). Ben-David, PDAs can operate gaming modes with Bluetooth and other wireless short range communication protocols. These PDAs seem to be in close function and nature to the system and method of Ma. They also offer a sleep mode to conserve battery life. Being able to communicate in both modes would greatly improve the convenience of the system. For example two users within close proximity could play games together or separately. And if one device is idling it could still be awaken to perform the needed duty of authentication. Therefore it would have obvious to one of ordinary skill in the art at the time of the invention to use the PDA's of Ben-David teaching in system of Ma because it adds to the level of user enjoyment and to the conversation of battery power. One of ordinary skill in the art knows the many features of PDAs and their ability to wirelessly communicate. Substituting various models would lead to predictable results.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Syed Zia/

Primary Examiner, Art Unit 2431